Lampi di Cassandra/ Attacco? No, menefreghismo

18 maggio 2017—Perché i media si ostinano da giorni a definire WannaCry un "attacco", contribuendo così a creare disinformazione e a…

Lampi di Cassandra/ Attacco? No, menefreghismo

Figure 1:

18 maggio 2017—Perché i media si ostinano da giorni a definire WannaCry un "attacco", contribuendo così a creare disinformazione e a fomentare il panico?

(401)—Cassandra e i media non sono mai andati molto d'accordo, ma c'è mancato poco che stavolta ne scrivesse positivamente, perché le prime coperture dell'*affaire* WannaCry, fatte la prima sera da Sky e Rai 3 erano discrete; poca enfasi, attenzione ai fatti, opinioni di intervistati abbastanza esperti.

Poi la frana. Dal giorno dopo "Il Più Grande Attacco Hacker Del Mondo" si è impossessato delle news in prima serata, e **annunciatori in orgasmo hanno iniziato a straparlare** facendo a gara tra chi seminava più allarmismo e chi seminava più disinformazione. E' continuato per giorni. Difficile dire chi ha vinto.

L'informazione e gli ascoltatori hanno certamente perso.

Cassandra doverosamente proverà a fare un po' di chiarezza sui punti principali, lasciando a persone più esperte come Matteo Flora riassumere i particolari tecnici e "storici."

Primo: non c'è stato nessun attacco.

Come il vocabolario Treccani insegna:

attacco s. m. (der. di attaccare) (pl. -chi). — (…) 3. Assalto con forze militari, azione offensiva svolta decisamente, con impeto e grande impiego di forze allo scopo di sopraffare e disorganizzare il nemico: preparare un a.; (…) Non c'è stato nessun attacco perché non esisteva nessun nemico da attaccare o da cui essere attaccati; solo una manica di cialtroni può definire attacco un'epidemia, anzi una pandemia di un malware.

E' avvenuta un'azione di criminalità informatica senza target precisi, del tutto usuale, che ha semplicemente assunto dimensioni maggiori (anche se non così tanto) del solito. E ha dimostrato forse che i sistemi informativi degli ospedali inglesi stanno peggio di quelli delle nostre ASL. L'obiettivo? Il solito, semplicemente fare soldi a spese di chiunque.

Secondo: il modus operandi dei criminali in questione e i mezzi usati sono del tutto ordinari.

Il ransomware/cryptoware con pagamento del riscatto via bitcoin è in giro da fine 2013, e ha colpito anche in Italia un sacco di persone. Davvero non avete un amico/conoscente/antani che se lo sia preso?

Terzo: c'è qualcosa di nuovo che ha reso questo malware così infettivo?

Si, c'è; il vettore di attacco è un (ex)zero day del protocollo SMB, che fa parte del malware rilasciato a marzo in Vault7.

Lasciate a Cassandra la soddisfazione di ricordare "Io ve l'avevo detto".

Non era difficile prevedere che la massiccia pubblicazione di malware battezzata "Vault7" avrebbe fornito mezzi nuovi e più potenti ai normali criminali informatici.

Perché allora nessuno se ne è (pre)occupato?Proprio a marzo Microsoft ha rilasciato una patch di questa vulnerabilità, quindi prima che WannaCry colpisse.

Patch ovviamente esistente e autoinstallata solo dalle versioni di Windows più recenti, lasciando indifese come un branco di agnelli a Pasqua una fetta cospicua delle installazioni di Windows collegate a Internet o anche solo in LAN.

Quarto: Di chi è la colpa?

Questa è facile; la colpa è delle aziende e degli enti che tengono in piedi sistemi informativi, anche critici, tagliando o azzerando anno dopo anno i budget per la sicurezza e per l'aggiornamento dei sistemi. Stavolta sarebbe bastato usare GNU/Linux, oppure installare le patch, oppure segregare in reti separate i sistemi Windows che non potevano essere aggiornati, oppure airgappare quelli appartenenti a sistemi o infrastrutture critiche.

Ma anche voi, voi che non fate i backup, che tenete tutti i dati in linea, che vi state riempiendo la casa di oggetti smart e di IoT il cui firmware non verrà mai aggiornato, che vi affidate al modem/router del provider o peggio acquistato e dimenticato, siete attori dello stesso film. Solo che non vi hanno ancora chiamato in scena.

Questa volta vi è andata bene. La prossima sarà peggio.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on October 31, 2023.

Canonical link

Exported from Medium on August 27, 2025.